Engineer

DHCP

protocole de prêt d'adresses IP et de paramètres aux hôtes

Ce que c’est

DHCP, pour Dynamic Host Configuration Protocol, permet à un appareil qui vient de rejoindre un réseau de connaître sa place sur ce réseau. Un portable connecté au Wi-Fi connaît son adresse matérielle et guère plus. DHCP lui fournit une adresse IP, le masque de sous-réseau, le routeur par lequel envoyer le trafic et les serveurs DNS à interroger, sans saisie manuelle. Le protocole est défini dans la RFC 2131, publiée en mars 1997, dont le résumé le présente comme un moyen de transmettre des informations de configuration aux hôtes d’un réseau TCP/IP. Il vient de l’ancien Bootstrap Protocol, BOOTP. Son principal ajout est l’attribution automatique d’adresses réutilisables.

La RFC 2131 distingue trois modes d’attribution. En attribution automatique, le client reçoit une adresse permanente. En attribution dynamique, il la reçoit pour une durée limitée ou jusqu’à ce qu’il la rende. En attribution manuelle, l’administrateur réseau choisit l’adresse et DHCP ne fait que la transmettre. Seule l’attribution dynamique permet à une adresse de revenir d’elle-même dans le pool lorsque son détenteur n’en a plus besoin. C’est le mécanisme traité dans la suite de cet article.

La période pendant laquelle une adresse est prêtée s’appelle un bail. Le client peut le prolonger, rendre l’adresse avant son terme et même demander un bail infini. La RFC note qu’un serveur peut néanmoins préférer des baux longs mais finis, afin de finir par constater qu’un client a été retiré du service. Derrière le serveur se trouve ce que la RFC appelle un stockage persistant : une entrée par client, indexée par un identifiant, qui conserve les paramètres qui lui ont été attribués.

DHCP utilise UDP. Les clients envoient leurs messages au port serveur 67 et les serveurs répondent sur le port client 68. Les options transmissibles par le serveur, du masque de sous-réseau à la durée du bail, sont spécifiées séparément dans la RFC 2132. IPv6 possède son propre protocole, DHCPv6, désormais spécifié dans la RFC 9915, une norme Internet de janvier 2026 qui a remplacé la RFC 8415. Il utilise d'autres ports, 546 pour les clients et 547 pour les serveurs et les agents relais, et peut remplacer l'autoconfiguration sans état des adresses, SLAAC, ou fonctionner à ses côtés. La RFC 9915 appelle elle-même le protocole IPv4 DHCPv4 lorsqu'il faut distinguer les deux. Elle consigne le consensus de l'IETF : la configuration IPv4 devrait passer par DHCPv4 plutôt que DHCPv6.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce que DHCP ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Du Wi-Fi, des pare-feu et des accès à distance configurés pour travailler de partout, en laissant entrer uniquement les personnes autorisées.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. 30 instances VPS Ubuntu Linux administrées — 30 serveurs Linux gérés, avec récupération prévue

30 instances VPS Ubuntu Linux administrées Contactez-nous →

Pourquoi c'est important

Chaque appareil d'un réseau a besoin du même petit ensemble de paramètres, et une seule valeur fausse suffit à le couper du réseau : un masque qui ne correspond pas au sous-réseau, une adresse de routeur appartenant à quelqu'un d'autre, un serveur DNS éteint l'an dernier. Sans DHCP, il faut saisir ces valeurs sur chaque appareil et veiller à leur exactitude à chaque changement. Avec DHCP, elles sont regroupées au même endroit. Changer le serveur DNS de tout un bureau revient alors à modifier la configuration du serveur plutôt qu'à faire le tour du bâtiment.

Le bail permet au protocole de passer à l'échelle. L'attribution dynamique prête les adresses pour une durée fixée ; un pool peut donc servir sur une semaine plus d'appareils qu'il ne contient d'adresses, à condition qu'ils ne soient pas tous présents en même temps. La RFC 2131 juge ce mode particulièrement utile pour les clients connectés temporairement et pour partager un pool limité entre des clients qui n'ont pas besoin d'adresse permanente. Comme un client peut simplement disparaître, le protocole ne compte pas sur ses adieux : la RFC précise que son bon fonctionnement ne dépend pas de l'envoi d'un message de libération par le client. L'adresse revient à l'expiration du bail, que son détenteur le signale ou non.

La durée du bail est donc un vrai choix de conception, pas une valeur prédéfinie à laisser intacte. Un bail long immobilise plus longtemps les adresses des appareils partis. Un bail court augmente le trafic de renouvellement et laisse moins de temps pour réparer un serveur qui ne répond plus : un client dont le bail expire avant qu'il puisse joindre un serveur doit cesser d'utiliser son adresse.

DHCP est aussi une question de confiance. La première réponse qu'un appareil accepte lui indique le routeur qui transportera tout son trafic et le serveur DNS qui traduira chaque nom recherché. Qui contrôle cette réponse contrôle donc les destinations de l'appareil. La RFC 2131 est explicite : sa section de sécurité qualifie le protocole, dans sa forme actuelle, de « très peu sûr », car il repose directement sur UDP et IP et parce qu'il est difficile d'équiper de mots de passe ou de clés les machines qu'il devait servir. La même section note qu'il est facile d'installer des serveurs non autorisés, capables de distribuer des adresses fausses ou en double et de faux routeurs ou serveurs de noms. La protection doit venir du réseau qui entoure le protocole, pas du protocole lui-même.

À quoi cela ressemble en pratique

Prenez un portable d'adresse matérielle 00-00-5E-00-53-2A qui rejoint le sous-réseau d'un bureau, 192.0.2.0/24, où une machine en 192.0.2.1 joue à la fois le rôle de routeur et de serveur DHCP. Le portable n'a initialement aucune adresse. Son premier message part donc de l'adresse source 0.0.0.0 et est diffusé à tous sur la liaison. Quatre messages plus tard, il est configuré :

```
portable 00-00-5E-00-53-2A                    serveur 192.0.2.1

1  DHCPDISCOVER  0.0.0.0 -> 255.255.255.255, port serveur 67
                 y a-t-il un serveur ici ?
2  DHCPOFFER     propose 192.0.2.50 pour 86400 s,
                 identifiant du serveur 192.0.2.1
3  DHCPREQUEST   diffusion : identifiant du serveur 192.0.2.1,
                 adresse demandée 192.0.2.50
4  DHCPACK       192.0.2.50 est attribuée au portable pour 86400 s
```

Un nombre quelconque de serveurs peut répondre à la découverte, et le client peut attendre de recueillir plusieurs offres. Il en choisit ensuite une et diffuse une requête qui nomme le serveur retenu dans l'option d'identifiant du serveur et demande l'adresse proposée par celui-ci. Tout autre serveur qui voit cette

diffusion la comprend comme un refus de sa propre offre. Le serveur choisi enregistre l'association dans son stockage et la confirme par un accusé de réception.

L'accusé de réception transporte les paramètres, chacun sous la forme d'une option numérotée définie dans la RFC 2132. Pour ce portable, il pourrait contenir :

```
option 53  type de message         5 (DHCPACK)
option 54  identifiant du serveur  192.0.2.1
option 51  durée du bail           86400 (secondes, un jour)
option 1   masque de sous-réseau   255.255.255.0
option 3   routeur                 192.0.2.1
option 6   serveurs DNS            192.0.2.53
```

La RFC 2132 exige que le masque de sous-réseau précède l'option de routeur lorsque les deux sont présents. Elle permet au serveur d'énumérer plusieurs routeurs et plusieurs serveurs de noms, par ordre de préférence. La durée du bail et l'identifiant du serveur ne sont pas facultatifs : la RFC 2131 les rend tous deux obligatoires dans l'accusé de réception d'une requête.

Avant d'utiliser 192.0.2.50, le client devrait vérifier que personne d'autre ne l'utilise déjà, par exemple avec ARP. Si l'adresse est prise, il doit envoyer DHCPDECLINE et recommencer. Sinon, les temporisateurs démarrent. À moins que le serveur n'envoie ses propres valeurs, T1 vaut la moitié du bail et T2 ses sept huitièmes. Pour un bail d'un jour :

```
t = 0 s        DHCPACK reçu, début du bail
t = 43200 s    T1: RENEWING, DHCPREQUEST en monodiffusion vers 192.0.2.1
t = 75600 s    T2: REBINDING, DHCPREQUEST diffusé à tout serveur
t = 86400 s    le bail expire : cesser d'utiliser 192.0.2.50, recommencer
```

La RFC demande une certaine variation aléatoire autour des deux temporisateurs, afin que tous les portables d'une salle allumés en même temps ne renouvellent pas leur bail à la fois. Si une requête reste sans réponse, le client attend la moitié du temps restant avant de réessayer, avec un minimum de 60 secondes. Un client qui fonctionne normalement renouvelle à mi-parcours et ne s'approche jamais de la fin de son bail.

Le serveur n'a pas besoin de se trouver sur le sous-réseau du portable. Un routeur peut agir comme agent relais : il reçoit la diffusion et la transmet à un serveur ailleurs. Sa propre adresse, inscrite dans le champ giaddr du message, indique au serveur où envoyer la réponse. La RFC 2131 compte sur ce mécanisme et note que les relais évitent d'avoir un serveur DHCP sur chaque segment réseau. À l'échelle décrite par notre page de prestations réseau et VPN, qui mentionne la configuration et le déploiement de 1 000 routeurs Wi-Fi et l'administration de l'infrastructure réseau de plus de 1 000 serveurs, saisir les adresses à la main n'est pas envisageable. L'organisation des pools, des baux et des relais devient un élément de la conception du réseau.

Où les problèmes surviennent

Un serveur non autorisé répond le premier. Un routeur domestique branché dans le mauvais sens, une machine de test reliée par pont au réseau du bureau ou un attaquant agissant délibérément peuvent tous répondre à un DHCPDISCOVER. Rien dans le protocole n'indique au client quel serveur est le vrai. La RFC 2131 énumère les risques : adresses fausses ou en double, orientation vers un faux routeur ou de faux serveurs de noms. Les commutateurs peuvent filtrer ces messages. La RFC 7610 note que la forme IPv4 de ce filtre, DHCP snooping, est largement déployée. N'autorisez les messages de serveur DHCP que sur les ports du commutateur qui mènent aux vrais serveurs ou relais, et rejetez-les partout ailleurs.

Le pool est épuisé. Un pool contient un nombre fixe d'adresses, et l'attribution dynamique ne les récupère qu'à la fin des baux. Sur un réseau invité où défilent des centaines de téléphones, un bail d'une semaine signifie que chaque visiteur de la semaine précédente conserve une adresse. La RFC 2131 prévient aussi qu'un client malveillant peut réclamer toutes les adresses et n'en laisser aucune aux autres. Dimensionnez le pool pour le nombre d'appareils présents sur la durée d'un bail et raccourcissez celui-ci là où les appareils vont et viennent.

Un nouveau sous-réseau sans relais. La découverte est une diffusion, et les diffusions s'arrêtent au routeur. Un nouveau VLAN ou étage sans agent relais configuré ne reçoit aucune réponse. Un hôte qui implémente la RFC 3927 peut alors s'attribuer une adresse locale au lien dans la plage 169.254/16. Elle ne fonctionne que sur cette liaison, car les routeurs ne doivent pas transférer de paquets provenant de ces adresses ou leur étant destinés. Configurez un agent relais sur le routeur de chaque sous-réseau ayant des clients DHCP et lisez une adresse 169.254 sur un client comme le signe qu'aucun serveur n'a répondu.

Deux serveurs en désaccord. Faire fonctionner deux serveurs pour la résilience est raisonnable, mais la RFC 2131 dit que tous devraient renvoyer les mêmes paramètres, hormis l'adresse elle-même, pour qu'un client se comporte pareil quelle que soit l'offre choisie. Elle confie à l'administrateur la responsabilité de cette cohérence. Deux serveurs aux plages qui se chevauchent peuvent aussi prêter la même adresse à deux clients. Donnez à chacun sa plage, gardez les mêmes options et comparez les deux après chaque changement.

Des adresses fixes dans le pool. Une imprimante recevant manuellement une adresse statique à l'intérieur de la plage prêtée par DHCP finira par entrer en conflit avec un bail. Le protocole tente de le détecter : un serveur devrait sonder une adresse avant de la réutiliser, par exemple avec une requête d'écho ICMP. Un client constatant que sa nouvelle adresse est déjà prise doit la refuser ; le serveur marque alors l'adresse comme indisponible et devrait avertir l'administrateur. Ce sont des filets de sécurité, qui ne remplacent pas un plan d'adressage. Gardez les adresses configurées à la main hors du pool, ou utilisez l'attribution manuelle pour que le serveur conserve lui-même la réservation.

IPv6 reste ouvert. Le filtrage de DHCPv4 n'agit pas sur DHCPv6, qui utilise d'autres ports et qu'un client peut démarrer lorsqu'une annonce de routeur indique que DHCPv6 est disponible. La RFC 9915 renvoie à la RFC 7610, DHCPv6-Shield, pour atténuer les risques de serveurs DHCPv6 non autorisés. La RFC 7610 précise que les annonces de routeur non autorisées sortent de son périmètre ; elles relèvent de Router Advertisement Guard. Filtrez les messages de serveur DHCPv6 sur les ports d'accès comme ceux de DHCPv4, et utilisez RA-Guard en parallèle.

Pour aller plus loin

- RFC 2131 : protocole de configuration dynamique des hôtes — le protocole lui-même : modes d'attribution, baux, échange de messages, temporisateurs T1 et T2 et section de sécurité.
- RFC 2132 : options DHCP et extensions fournisseur de BOOTP — chaque option numérotée, du masque de sous-réseau et de la liste de routeurs à la durée du bail et au type de message.
- RFC 9915 : protocole de configuration dynamique des hôtes pour IPv6 (DHCPv6) — le protocole IPv6, ses ports, ses messages et son fonctionnement avec SLAAC ; il remplace la RFC 8415.
- RFC 7610 : DHCPv6-Shield, protection contre les serveurs DHCPv6 non autorisés — filtrage des messages serveur au commutateur, précédent IPv4 de DHCP snooping et ce qui relève de RA-Guard.

- RFC 3927 : configuration dynamique des adresses IPv4 locales au lien — les adresses 169.254/16 qu'un hôte peut s'attribuer lorsqu'aucun serveur ne répond, et pourquoi les routeurs ne transfèrent jamais les paquets vers ou depuis ces adresses.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Qu'est-ce que DHCP ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/dhcp/